Payment Card Industry (PCI) Compliance Policy

Office of Budget and Finance

March 2021

Table of Contents

I. OVERVIEW

In 2006, the major credit card companies (American Express, Discover Financial Services, JCB, Visa International, and MasterCard Worldwide) formed the Payment Card Industry Security Standards Council (PCI-SSC) and established the Payment Card Industry Data Security Standard (PCI-DSS), a set of operating and technical compliance requirements, to address the security concerns resulting from the widespread use of payment cards. Merchants, such as CUNY and its Related Entities, must comply with these standards regardless of the size of the institution and/or the number of payment card transactions handled. Complying with the PCI-DSS will help protect Cardholder Data (see Appendix A for definition of Cardholder Data). This document sets forth the University's policy for complying with the PCI-DSS.

At a high level, the PCI-DSS is comprised of six categories and twelve requirements[1]. PCI-DSS requirements (see Appendix C) are dependent on an organization's merchant level (see Appendix B). PCI-DSS compliance is a continuous process. The University will be judged by its compliance with each of the requirements at all times and not at a particular moment in time. The University shall assess, remediate, and report its compliance status on an on-going basis.

While the law does not mandate PCI-DSS compliance, non-adherence to PCI-DSS can subject the University to significant financial and reputational risks. Failure to comply can result in: a) fines and penalties imposed by payment card institutions and banks; b) monetary costs associated with legal proceedings, settlements and judgements; and c) suspension of the merchant account and the inability to accept payment cards for payment.

II. PURPOSE

The purpose of this Policy is to provide the University with clear and manageable steps to protect customer Cardholder Data and to protect the University from a cardholder breach by complying with PCI-DSS.

III. ROLES AND RESPONSIBILITIES

The University is committed to safeguarding personal information conveyed in processing payment (debit and credit) card payments. The University shall be PCI-DSS compliant and use secure methods to process payment card transactions to serve its students and the broader CUNY community. The Central Office is responsible for ensuring that University-wide vendors and systems are PCI-DSS compliant. Colleges and Related Entities are responsible for ensuring that their local vendors and systems are compliant. Related Entities must provide validation of their compliance to their supported College and/or the University. CUNY PCI Liaisons have been appointed at each College and shall be the point persons for all PCI related tasks and activities. College and Central Office management are responsible for maintaining and overseeing compliance with this Policy within their line responsibilities.

[1] There are over 200 sub requirements to the 12 primary requirements. Please refer to the respective PCI-DSS requirements for the specific details.

IV. SCOPE

This Policy applies to the Colleges and Related Entities that have access to Cardholder Data and to the people, processes and technology that handle Cardholder Data at or on behalf of CUNY. This includes, but is not limited to, any CUNY College, department, office, employee (full-time, part-time and temporary), student, vendor, software, computer, and/or electronic devices, involved in processing Cardholder Data on behalf of CUNY.

V. DEFINITIONS

"College" means a constituent unit of the University, including without limitation senior and community colleges, graduate and professional schools, Macaulay Honors College, and the Central Office, as well as fund groups and organizations that are not legally separate from the University (e.g., the Queens College Athletic and Recreational Fund, the college associations of Hunter College, the School of Professional Studies and the Graduate School of Public Health and Health Policy).

"CUNY" and "University" mean The City University of New York.

"Related Entities" means the following types of entities and their subsidiaries, if legally separate from the University: foundations, alumni associations, auxiliary enterprise corporations, college associations, student services corporations, childcare centers, performing arts centers, and art galleries, that accept payment cards using technology owned, operated or made available by a College and/or the University, such as servers, networks, hardware and software, and/or are using the name or a trademark of CUNY or a constituent unit of CUNY, in connection with its operations.

"Payment card" means a debit or credit card.

For list of PCI-DSS related definitions, see Appendix A.

VI. GENERAL REQUIREMENTS AND PROCEDURES

A. Storage of Sensitive Authentication Data and Cardholder Data

Storage of electronic and/or physical Cardholder Data or Sensitive Authentication Data poses significant risks and increases the number of requirements that must be satisfied to be PCI-DSS compliant.

PCI-DSS prohibits the storage of Sensitive Authentication Data, even if the data is encrypted. Sensitive Authentication Data includes the full contents of any data on a card's magnetic stripe, card verification codes or values (CVC/CVV) and personal identification numbers (PIN).

Electronic and physical Cardholder Data shall not be stored unless there is a justified business need to do so. Each College and Related Entity wishing to store Cardholder Data, specifically full Primary Account Numbers (PANs), shall define and document the business need for storage, including maintaining a list of all roles that require access to full PANs and staff who have such roles. Documentation must be kept up-to-date and readily available in the event of an audit. Notwithstanding the foregoing, the following Cardholder Data may be retained after a transaction is successfully processed for the retention period described in this Policy: payment cardholder name, transaction authorization number, transaction date, and transaction dollar amount.

B. Access to Cardholder Data

Cardholder Data is classified as confidential data under the CUNY Data Classification Standard. Access to Cardholder Data shall be restricted to those individuals whose job responsibilities require such access, on a strict need to know basis, as per CUNY IT Security Procedures, Section II, Access Issues. This includes full-time, part-time, temporary, or contracted College or Related Entity employees. Offices and departments that handle Cardholder Data shall define and document the roles and responsibilities of those individuals whose job functions require them to access Cardholder Data. It is crucial that individuals with Cardholder Data-handling job functions are instructed to not disclose any Cardholder Data, unless deemed necessary by a supervisor in accordance with PCI-DSS requirements and CUNY policies.

C. Protecting Stored Cardholder Data

Colleges and Related Entities with a justified business need to store Cardholder Data must ensure that Cardholder Data is appropriately protected. If there is a justified business need, the cardholder's name, PAN, expiration date, and service code may be stored if protected in accordance with PCI-DSS requirements. Masking the PAN anywhere it is displayed, such as on receipts, so that only the first six and/or the last four digits are displayed is one method of protecting stored Cardholder Data. Other methods include encryption or truncation.

D. Retention of Cardholder Data

Any Cardholder Data that must be retained after transaction authorization on the basis of a documented and justified business need must be kept secured and only accessible by those whose job requires that they have access to the data. For physical media containing Cardholder Data, for example, the media should be stored in a filing cabinet or safe that is locked at all times (during and after business hours).

Card Verification Codes or Values (CVC/CVV) and Personal Identification Numbers (PINs) must never be retained.

Cardholder Data shall not be retained for more than one year. Colleges and Related Entities shall determine a quarterly process for identifying and securely deleting stored Cardholder Data at the end of its retention period.

E. Disposal of Cardholder Data

Except for Cardholder Data being retained based on a justified business need, any Cardholder Data captured to process a transaction shall be purged, deleted, or destroyed, in an irretrievable manner, immediately after authorization. The following are approved techniques for disposing of Cardholder Data:

- Paper shall be shredded, using a crosscut shredder, pulped, or incinerated.
- Digital storage media, such as CDs, DVDs, Disks, USB Drives, etc. must be securely overwritten or physically destroyed in a manner that prevents unauthorized disclosure, as per PCI-DSS requirements and the CUNY IT Security Procedures.

Cardholder Data awaiting disposal must be stored in a secure container with a lock to prevent access. The container must be labeled "classified" or have a similar label to indicate the sensitivity of the data.

F. Receipt of Cardholder Data via End-User Messaging Technologies

Colleges and Related Entities shall not accept Cardholder Data via end-user messaging technologies (i.e., email, instant message, text message, etc.), which are not a secure means of transmission. All forms and other documents that collect Cardholder Data shall exclude email and/or cell phone number fields as a method of submission. Cardholder Data may be accepted by fax if the machine does not store the data in memory, converts the fax into email, or is not connected to the local network (i.e., a dedicated fax machine).

If an office or department receives Cardholder Data via end-user messaging, the message shall be deleted. The office or department should compose a new email or text message to the sender advising them to refrain from sending Cardholder Data through this means of communication and provide proper credit card submission instructions. Cardholder Data received through end-user messaging shall not be processed.

G. Self-Assessment Questionnaire (SAQ)

Each College and Related Entity department or office that processes payment card transactions shall complete an SAQ (see Appendix D) annually to demonstrate its compliance with PCI-DSS. The College PCI Liaisons shall be the point persons for additional information on submitting an SAQ.

H. Internal and External Vulnerability Scans

Each College and Related Entity that stores, processes, or transmits Cardholder Data through a CUNY network must conduct internal and external vulnerability scans, at least on a quarterly basis and after any significant changes, as required by the PCI-DSS. A PCI-validated Approved Scanning Vendor must conduct external vulnerability scans. For additional information, refer to Internal and External Vulnerability Scanning Procedures.

I. Third-Party Vendor and Service Provider Compliance

Third-party vendors and/or service providers that store, process, or transmit Cardholder Data on behalf of a College or Related Entity can impact the security of the University and must be PCI-DSS compliant. Colleges and Related Entities shall establish a process for engaging third-party vendors and/or service providers, including confirming the third party's PCI compliance status by checking the appropriate database (i.e., the VISA Global Registry).

All Colleges and Related Entities utilizing a third-party vendor and/or service provider shall maintain an up-to-date list of all vendors and/or service providers, including a description of the services provided and the type of data shared with the third party.

Due to evolving PCI standards, Colleges and Related Entities must verify the PCI compliance status of third parties by requesting and reviewing an Attestation of Compliance (AOC), annually.

J. Access to System Components containing Cardholder Data

Colleges and Related Entities utilizing a system component handling Cardholder Data (i.e. Virtual Terminal or payment processing platform) shall assign a unique ID or username to each person with access and add and remove a person's access as needed. Access for users who separate from the University or whose job responsibilities no longer require such access shall be immediately revoked and removed. Colleges and Related Entities shall ensure that all users secure their accounts with strong passwords, that are changed at least every 90 days. As per PCI-DSS requirements, passwords must, at least, meet the following parameters:

- A minimum password length of at least seven characters
- Contain both numeric and alphabetic characters

Colleges and Related Entities shall not use generic or shared user IDs and passwords and shall remove all generic user IDs prior to the utilization of the system component.

K. Point-of-Sale (POS) Devices and Protection against Skimming and Tampering

Point-of-Sale (POS) devices that are purchased or owned by a College or Related Entity are in-scope for PCI compliance. PCI-DSS requirements call for the protection from tampering and skimming of devices that capture payment card data via direct physical interaction. Departments or offices utilizing a Point-of-Sale (POS) device that is purchased or owned shall maintain an up-to-date device inventory log, which includes the device name, model, serial #, and location of device, and shall periodically inspect the device for signs of skimming and tampering, as required by the PCI-DSS (see CUNY POS Device Inspection Guidelines and Checklist).

L. Disposition of Point-of-Sale (POS) Devices

Colleges and Related Entities with Point-of-Sale devices or terminals that have been inactive for over two years shall dispose of the devices (see CUNY POS Device Inspection Guidelines and Checklist).

M. Protection of Networks and Systems

Colleges and Related Entities shall establish and implement methods for protecting networks and systems that process, store, or transmit Cardholder Data, including but not limited to testing all network connections and changes to firewall configurations, maintaining network diagrams, using strong cryptography, maintaining up-to-date and actively running anti-virus programs and updating security patches in a timely manner, as required by PCI-DSS. Efforts should be made to limit and reduce the scope of required compliance with PCI-DSS by isolating and segmenting areas of the network and systems used to process Cardholder Data. Colleges and Related Entities shall refer to the CUNY Information Technology Security Procedures for additional requirements.

N. Annual PCI Awareness Training

All College and Related Entity staff with access to Cardholder Data shall take the PCI Awareness course, offered by the University PCI Compliance Office, upon hire and at least annually thereafter.

VII. Fraud Reporting Procedures

Colleges and Related Entities shall follow CUNY's breach reporting procedures in the event of any alleged fraudulent or criminal activity:

a. CUNY's 2020 Protocol for Reporting Allegations of Corruption, Fraud, Criminal Activity, Conflicts of Interest or Abuse
b. Breach of Private Information Procedure
c. Notify the University PCI Compliance Office (PCIcompliance@cuny.edu)

VIII. Policy Implementation and Amendments

Any proposed exceptions to this Policy must be approved in writing by the Senior Vice Chancellor and Chief Financial Officer, or their successors or designees, after consultation with the Offices of the General Counsel and Information Security.

The Colleges and Related Entities shall comply with any procedures, manuals, memoranda, directives, and the like that relate to this Policy and were issued prior to or following the effective date of this Policy by the University including by the Office of Budget and Finance, the Office of the General Counsel, and/or the Office of Information Security.

Except for modifications, supplements or updates necessitated by changes in law, regulations, or administrative requirements; or for consistency with other University policies, the CUNY Board of Trustees must approve any proposed amendments to this Policy. The CUNY Office of Budget and Finance will be responsible for the periodic review of this Policy, as well as ensuring that all appropriate parties are informed of them.

IX. HELPFUL RESOURCES

CUNY PCI Compliance Webpage:
www.cuny.edu/pcicompliance

CUNY Information Technology Security Procedures:
https://www.cuny.edu/security-policies-procedures/IT-Security-Procedures-6-25-2014.pdf

CUNY Data Classification Standard:
https://www.cuny.edu/security-policies-procedures/Data-Classification-Standard-CUNY-2019-8-19a.pdf

CUNY Protocol for Reporting Allegations of Corruption, Fraud, Criminal Activity, Conflicts of Interest or Abuse:
https://www.cuny.edu/Updated-CUNY-IG-Fraud-Reporting-Protocols-2020.pdf

CUNY Breach of Private Information Procedure:
https://www.cuny.edu/security-policies-procedures/BreachReportingProcedureV07182006.pdf

PCI Data Security Standards:
https://www.pcisecuritystandards.org/

PCI-DSS Document Library:
https://www.pcisecuritystandards.org/document_library

PCI-DSS v3.2.1:
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

PCI-DSS Requirements and Self-Assessment Questionnaires:
https://www.pcisecuritystandards.org/document_library?category=saqs#

PCI Validated Approved Scanning Vendors:
https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors

PCI Validated Qualified Security Assessors:
https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

List of third-party service providers per Visa that are PCI Compliant:
https://www.visa.com/splisting/searchGrsp.do

Appendix A: PCI-DSS DEFINITIONS

Payment Card Industry Security Standards Council (PCI-SSC) was founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa Inc., whose mission is to enhance global payment account data security by developing standards and supporting services that drive education, awareness, and effective implementation.

Payment Card Industry Data Security Standards (PCI-DSS) refers to a set of technical and operational requirements established by the PCI-SSC designed to protect account data and applies to all entities involved in payment card processing – including merchants, processors, acquirers, and service providers.

Merchant means any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa).

Payment card(s) mean credit and debit cards bearing the logo of major card brands, including Visa, MasterCard, American Express, Discover and JCB used to make a payment.

Card Verification Value (CVV2 or CVV) is a three-digit number on the back or four-digit number on the front of a payment card. PCI does not permit the CVV2/CVV to be stored on paper, electronically, or by any other means.

Cardholder Data Environment (CDE) refers to the people, processes and technology that store, process, or transmit Cardholder Data or sensitive authentication data, including any connected system component.

Cardholder Data (CHD) is any personally identifiable information (PII) associated with a person who has a credit or debit card. Cardholder Data includes the primary account number (PAN), which consists of a customer's 16-digit payment card number along with any of the following data types: cardholder name, expiration date, and card verification value.

Personal Identification Number (PIN) is the personal number used in debit card transactions.

Sensitive Authentication Data is the full magnetic stripe data (Track Data) including chip and PIN. The data encoded in the magnetic stripe used for authorization during transactions when the card is presented as well as the chip and PIN data. This data must be purged and never kept after transaction authorization including the service code, card validation value, code, and proprietary reserved value.

Payment Application is approved software sold, distributed, or licensed which stores, processes, or transmits Cardholder Data as part of authorization or settlement. This includes customized, pre-installed, and "off-the-shelf" software.

Point of Interaction (POI) is the initial point where data is read from a card. An electronic transaction-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a card transaction. The POI may be attended or unattended. POI

transactions are typically integrated circuit (chip) and/or magnetic-stripe card-based payment transactions.

Point of Sale (POS) Hardware and/or software used to process payment card transactions at merchant locations.

PIN Entry Device (PED) is a terminal that allows entry of a customer's PIN.

Third-Party Vendor (also called "third-party service provider") are business entities directly involved in transmitting, processing, or storing of Cardholder Data or which provides services that control or could impact the security of Cardholder Data.

Virtual Payment Terminals are web-browser-based access to a third-party service provider website to authorize payment card transactions when the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment.

Self-Assessment Questionnaire (SAQ) refers to questionnaires listing the PCI Data Security Standards that apply to each method of processing payment cards.

Attestation of Compliance (AOC) is a report to attest to the results of a PCI-DSS assessment and can be requested from a third-party vendor.

Level 1 Service Provider is a vendor that provides access to the internet and to applications to facilitate the transfer and/or storage of payment card information. The following link provides a complete list of PCI Compliant Level 1 Service Providers: http://www.visa.com/splisting/searchGrsp.do.

Approved Scanning Vendor (ASV) refers to a company qualified by the PCI Security Standard Council to conduct external vulnerability scanning services in accordance with PCI-DSS.

Qualified Security Assessor (QSA) is a PCI assessor validated and listed by the PCI Security Standards Council's. List of QSAs:
http://pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

Appendix B: Merchant Levels

Level	Amex	Discover	JCB	MasterCard	Visa
1	Merchants processing over 2.5 million AMEX transactions annually or any merchant that American Express deems a level 1	Merchants are currently not categorized into levels based on transaction volume. Discover takes a risk based approach for validating compliance.	Merchants processing over 1 million JCB transactions annually or compromised merchants	Merchants processing over 6 million MasterCard transactions annually or identified by another payment card brand as level 1, or merchants that have experienced an account data compromise	Merchant processing over 6 million Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system
2	Merchants providing 50,000 to 2.5 million AMEX transactions annually or any merchant that American Express otherwise deems level 2	N/A	Merchants processing less than 1 million JCB transactions annually.	Merchants processing 1 million to 6 million MasterCard transactions annually	Any merchant processing 1 million to 6 million Visa transactions per year
3	Merchants processing less than 50,000 AMEX transactions annually	N/A	N/A	Merchants processing 20,000 to 1 million MasterCard e-commerce transactions annually	Any merchant processing 20,000 to 1 million Visa e-commerce transactions per year
4	N/A	N/A	N/A	All other MasterCard Merchants	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants - regardless of acceptance channel - processing up to 1 million Visa transactions per year

Appendix C: Merchant Level Requirements

Level	Amex	Discover	JCB	MasterCard	Visa
1	Annual onsite review by QSA (PCI DSS Assessment) and Quarterly Network Scan by ASV	Quarterly Network Scan by ASV AND one of the following: Annual onsite review by QSA-PCI DSS assessment Annual Self Assessment Questionaire	Annual onsite review by QSA (PCI DSS Assessment) and Quarterly Network Scan by ASV		
2	Quarterly Network Scan by ASV	Annual Self Assessment Questionaire and Quarterly Network Scan by ASV			
3	Quarterly Network Scan by ASV	Quarterly Network Scan by ASV AND one of the following: Annual onsite review by QSA-PCI DSS Assessment Annual Self Assessment	N/A	Annual Self Assessment Questionaire and Quarterly Network Scan by ASV	
4	Quarterly Network Scan by ASV	N/A	Annual Self Assessment Questionaire and Quarterly Network Scan by ASV		

Appendix D: Self-Assessment Questionnaires (SAQs)

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Not applicable to face-to-face channels. Shopping Cart - your customers enter their credit card information into a website to make an online purchases, payments, or donations: a) all e-commerce page including all payments acceptance and processing are delivered directly from a 3rd party PCI-validated service provider or b) during the payment process, the consumer browser is redirected to a checkout/payment page (URL or iFrame) that is entirely controlled by a PCI-compliant 3rd party service provider.
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Applicable only to e-commerce channels. Shopping Cart - your customers enter their credit card information into a website to make an online purchases, payments, or donations: a) during payment process, the consumer's browser is redirected to a checkout/payment page (URL or iFrame) that is controlled by PCI-compliant third party service provider, but some elements (javascrip, CSS, etc.) are passed from the merchant page to the 3rd party payment page or b) the checkout/payment page directly posts payment information from the merchant website to a 3rd party service provider, but the page resides in the merchant website.
B	Merchants using only: • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. Not applicable to e-commerce channels.
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. Not applicable to e-commerce channels.
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. Not applicable to e-commerce channels. You use a web browser on a computer or mobile device to access a merchant services site for entering and authorizing credit card purchases. You should have a username and password and be able to access the site from any online computer. You never swipe the card, but instead use a keyboard or keypad to manually type in the credit card information
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. Not applicable to e-commerce channels. You are using Point of Sale (POS) software installed on a computer or other device. Computers with POS software are often combined with devices such as cash registers, bar code readers, printers, optical scanners, and card readers or you have a credit card reader connected to your computer that reads the card information and enters it into the virtual terminal.
P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. Not applicable to e-commerce channels.
D	All merchants not included in descriptions for the above types. Your customers enter their credit card information into a website to make an online purchases, payments, or donations. During the payment process, the consumer enters credit card information on a checkout/payment page that is part of the merchant website.